0849 Vol 1 #2

NUREG/CR-0849, Vol. 1, No. 2
UCRL-52715-80-2

Safeguards Material Control and Accounting Program: Quarterly Report, January–March 1980

Andrew J. Poggio and Donald R. Dunn

Prepared for
U.S. Nuclear Regulatory Commission

NEWARK PUBLIC LIBRARY
NOV 29 1980
U. S. GOVT. PUBS.
DEPOSITORY 376

LAWRENCE LIVERMORE LABORATORY

READEX FICHE

Y3.N88:25

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-0849, Vol. 1, No. 2
UCRL-52715-80-2
RS

Safeguards Material Control and Accounting Program: Quarterly Report January–March 1980

Manuscript Completed: September 1980
Date Published: October 1980

Prepared by
Andrew J. Poggio and Donald R. Dunn

Lawrence Livermore Laboratory
7000 East Avenue
Livermore, CA 94550

Prepared for
SAFER Division
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN No. A-0115

FOREWORD

This work was supported by the U.S. Nuclear Regulatory Commisssion (Office of Nuclear Regulatory Research) under a Memorandum of Understanding with the United States Department of Energy. The NRC FIN number is A-0115.

The scientific editors, A.J. Poggio and D.R. Dunn, wish to acknowledge the work of those individuals responsible for each section listed below:

2.0	Application and Further Development of Automated Safeguards Assessment Tools	D. W. Freeman W. J. Orvis A. A. Parziale C. J. Patenaude A. J. Poggio P. S. Wahler
3.0	Development of Value-Impact Methodology	R. Al-Ayat J. M. Huntsman** B. R. Judd**
4.0	Development of Improved Guidance Capabilities for MC&A Systems	P. D. Chilton* D. R. Dunn G. Kufahl* J. L. McDonnel* A. A. Vergari*
5.0	Analysis of the Role of an Interfacility SNM Accounting System for NRC Safeguards Assurance	D. R. Dunn J. L. McDonnel* R. K. Mullen*

* Advanced Technology Associates (ATA) Inc., Dublin, California

**Applied Decision Analysis (ADA) Inc., Menlo Park, Ca.

TABLE OF CONTENTS

Foreword iii
Abbreviations vii
Abstract ix
1.0 Introduction 1
2.0 Application and Further Development of Automated Safeguards Assessment Tools 2
2.1 Comparison of Data Requirements of LSD and SFC Guide 2
2.2 LLNL Assessment Technology Transfer 4
2.3 Update and Upgrade of the Structured Assessment Approach 5
3.0 Development of Value-Impact Methodology 9
4.0 Development of Improved Guidance Capabilities for MC&A Systems . . . 13
5.0 Analysis of the Role of an Interfacility SNM Accounting System for NRC Safeguards Assurance 18
6.0 References 20

ABBREVIATIONS

CCTV	Closed Circuit Television
DOE	Department of Energy
GMMA	Generic Minimal Material Accounting
ICP	Item Count Procedure
LLNL	Lawrence Livermore National Laboratory
LSD	Licensee Submittal Document
MA	Material Accounting
MAF	Material Accounted For
MC&A	Material Control and Accounting
MUF	Material Unaccounted For
NMMSS	Nuclear Material Management Safety and Safeguards
NRC/NMSS	Nuclear Regulatory Commission/Nuclear Material Systems and Safety
NRC-RES	Nuclear Regulatory Commission Office of Research
SAA	Structured Assessment Approach
SFC	Standard Format and Content
SNM	Special Nuclear Material
SSNM	Strategic Special Nuclear Materials
SSRS	Safeguards Status Report System
SVAP	Safeguards Vulnerability Analysis Program

ABSTRACT

This report summarizes the activity of the Safeguards Material Control and Accounting Program (MC&A) during the January-March 1980 quarter, conducted for the U.S. Nuclear Regulatory Commission at Lawrence Livermore National Laboratory. Described is progress made in the continued development of the Structured Assessment Approach (SAA) vulnerability methodology, particularly in preparing a user-oriented input-output interface and reducing the SAA's computer resource requirements. Also, a newly initiated technology transfer effort in which the NRC staff participated is detailed. Work continued in developing a value-impact methodology that focused on modeling alarm resolution; specifically, the procedures developed for eliciting the frequencies of false alarms are described. Additional support of the MC&A Upgrade Rule development, namely, analyzing the vulnerabilities of a generic minimal material accounting system to establish guidelines and checks and balances to prevent data falsification, is presented and a graphical procedure used in this effort is described. The report concludes with a brief description of the initial work performed in analyzing the role of an interfacility accounting system for safeguards assurance.

1.0 INTRODUCTION

The Lawrence Livermore National Laboratory (LLNL) Material Control Safeguards Evaluation Program for FY80, under the auspices of the U.S. Nuclear Regulatory Commission Office of Research, is directed in two main areas: 1) application and further development of automated safeguards assessment tools, and 2) assistance in the development of guidance for the forthcoming Material Control and Accounting (MC&A) upgrade rule.

During the first quarter of FY80 two automated vulnerability assessment tools were delivered to the NRC, the Structured Assessment Approach (SAA) and the Safeguards Vulnerability Analysis Program (SVAP).

This quarter's work with respect to automated safeguards assessment tools has focused entirely on the SAA and is described in Section 2.0. Particular emphasis is placed on three issues: 1) the evaluation and comparison of the information requirements of the SAA Licensee Submittal Document and the Standard Format and Content Guide of the Physical Protection Upgrade Rule Guidance Compendium, 2) the transfer of automated assessment technology from LLNL to NRC, and 3) the upgrade of the SAA to improve the user interface and to reduce the computer resource requirements.

In addition to the detailed assessment effort, a significant portion of our FY80 program plan has been devoted to technical support of the NRC in the development of the MC&A Upgrade Rule. The LLNL work in the Aggregated Systems Model (ASM) has made contributions in this area. Section 3.0 contains a summary of the ASM work with respect to modeling the response/resolution process for alarms, including false alarms, generated by an MC&A system. Further supporting work for the MC&A Upgrade Rule is presented in Sections 4.0 and 5.0. The current LLNL effort to develop guidance for protecting material accounting data from falsification is described in Section 4.0. This work is a follow-on to a previous task devoted to a systematic evaluation and critique of current material accounting regulations[1,7]. Section 5.0 describes the initial LLNL effort to analyze the actual and potential value of an interfacility NRC material accounting system.

2.0 APPLICATION AND FURTHER DEVELOPMENT OF AUTOMATED SAFEGUARDS ASSESSMENT TOOLS

Contributors: D. W. Freeman, W. J. Orvis, A. A. Parziale, C. J. Patenaude, A. J. Poggio, and P. S. Wahler.

The work performed during this quarter focused primarily on issues associated with the Structured Assessment Approach (SAA). The efforts were concentrated in 1) studying the data requirements of the SAA License Submittal Document and of the Physical Protection Fixed Site Upgrade Rule Standard Format and Content Guide, 2) initiating the transfer of the SAA technology and capabilities to the NRC, and 3) continuing the updating and upgrading of the SAA to improve its efficiency and to simplify the user interface.

2.1 COMPARISON OF DATA REQUIREMENTS OF LSD AND SFC GUIDE

Several questions were raised during a briefing at NRC on October 31, 1979, by NRC/NMSS staff regarding the data requirements of the SAA. As a result, an effort was undertaken to compare the data requirements of SAA and those of the Physical Protection Upgrade Rule Guidance Compendium Standard Format and Content Guide. This effort, started during the October-December 1979 quarter, was completed during this present quarter. The documentation used to define the data requirements were the SAA Licensee Submittal Document (LSD) and the NRC/NMSS Fixed Site Upgrade Rule Guidance Compendium, Standard Format and Content (SFC) Guide, pertaining to Part 73 Physical Protection Upgrade Rules.[2,3]

The objectives of this effort were to determine which information regarding the facility and the safeguards system was elicited by the LSD but not by the SFC Guide, and to estimate the limitations imposed upon an SAA assessment by deficiencies. When differences in data format and organization between the LSD and SFC Guide had a significant impact on performing an assessment, we included them in our study as well.

The results, conclusions, and recommendations presented here are based upon a comparison between the SAA (Version 1, October 1979 status) and the

December 21, 1978, NRC draft of the Fixed Site Upgrade Rule Guidance Compendium and recent revisions to that draft report entitled Attachment A, "Sample Portion of Security Plan" dated September 19, 1979, and Appendix I, "Component List Information Request Sheets" dated October 5, 1979. We concentrated on the review of Attachment A and Appendix I because they were more current. The results of the study are summarized in the following statements. For a more detailed discussion, the reader is referred to Ref. 4.

The most significant deficiencies in the SFC Guide information requirements, when viewed in the context of the SAA LSD requirements, are:

- SNM piping system information is absent.
- Safeguards system interconnectivity information is incomplete.
- Signal transmission and utility system information is incomplete.
- Probabilistic information is incomplete.

The impact of these SFC Guide information deficiencies upon performing an SAA assessment are:

- A fairly thorough SAA Level 1 (diversion path coverage) analysis is possible.
- At least partial SAA Level 2 (adequacy), Level 3 (sensitivity), and Level 4 (tampering) analyses are possible.
- Significant and critical safeguards vulnerabilities will be missed because of lack of input data as obtained from the SFC Guide.
- Reorganizing and reformatting the SFC Guide input data and information would simplify and expedite an automated assessment.

In light of the independent, parallel development of the SFC Guide and the SAA LSD, each addresses surprisingly similar information. Also, new NRC initiatives regarding information requests, especially recent revisions to the SFC Guide, appear to be in the appropriate direction for performing a comprehensive SAA automated vulnerability assessment.

2.2 LLNL ASSESSMENT TECHNOLOGY TRANSFER

The primary reason for an effort directed towards transferring LLNL automated assessment technology is to provide the NRC with a more directly accessible assessment tool, as well as to improve the usefulness of the tool through changes initiated by NRC personnel.

The initial work in the technology transfer effort was concentrated on the standard format and content of input data required by the License Submittal Document (LSD) used in performing a facility evaluation with the Structured Assessment Approach (SAA).

In January 1980 personnel from both NRC and LLNL decided to conduct a technology transfer meeting and to use a specified licensed nuclear facility as a vehicle. LLNL and NRC personnel understood at that time that, in order to achieve a successful transfer, both groups would need to actively participate as required. The initial meeting was held during the period 11-15 February 1980 and was attended by A. A. Parziale of LLNL and R. Shepard and E. McAlpine of NRC, each of whom devoted full time to the effort. The meeting was successful to the extent that the NRC personnel were fully instructed on how to compile the information required to perform an automated assessment of the physical security and material containment safeguard system using the specified facility (SLIP) as an example.

During the meeting all necessary information was compiled in diagrammatic form. The rules for tabulating and recording the input data were successfully transferred to the NRC analysts for completion of the input data generation task. It was agreed that in the days immediately following the meeting the NRC personnel would independently tabulate the specified facility data, compare the data files for purposes of validation, then send the information to LLNL for automated assessment. The results were then to be forwarded to

the NRC at a second technology transfer meeting and the exercise would be repeated for the material accounting system. Due to some unforeseen circumstances, the data for the physical security system could not be provided by the NRC until April 1980.

2.3 UPDATE AND UPGRADE OF STRUCTURED ASSESSMENT APPROACH

During this quarter our work has been concentrated on the input data collection system and the detailed tamper analysis code for the SAA.

2.3.1 Input Data Collection System

One of the primary goals of the SAA upgrade effort is to make the computer program more user-oriented, i.e., to improve the interface between the user and the data processing portion of the code. This requires modifications to the input and output portions of the code as well as additional aids for guiding the user in collecting data. Presently the LLNL effort is concentrated in improving the input portion of the code and in preparing a data collection handbook.

A Tektronix 4054 minicomputer has been used as an aid for data collection and for performing some preprocessing operations for the Safeguards Vulnerability Analysis Program (SVAP). This minicomputer will be employed in a similar manner for the SAA. Since performing the entire SAA vulnerability assessment on LLNL's computers, the CDC-7600's, has proven to be somewhat inefficient, a Tektronix 4054 will be used as an input aid. Thus NRC personnel will be able to collect data and check errors on NRC minicomputers before performing an SAA analysis on the CDC-7600's.

During this quarter, we established the general requirements of the computer code to be used on the Tektronix 4054. This code will guide and perform many of the input data collection and preparation tasks, such as reading input data, constructing a master data base, checking for inconsistencies and typographical errors, causing data set reports to be printed, presenting various options for adversary characteristics and goals to the operator, and some preprocessing of the input data.

During the coming quarter, we plan to complete the design and implementation of the data collection system on the Tektronix 4054 system.

2.3.2 Tamper Analysis Code

The SAA tamper analysis code performs an exhaustive analysis of the connections between all components in the physical security and material control and accounting systems. The components of these systems are locations, personnel, monitors, SSNM, time spans, accounting reports, and all other elements needed to describe a working model of the facility. For the purpose of the tamper assessment the relationship or connections between these components make up a directed graph which the computer stores as a matrix. Each component is represented on this graph or matrix by one node. The SAA finds all paths across this graph by computing a reachability matrix.[5] The reachability matrix approach helps determine those methods by which an individual or set of individuals could tamper with components to defeat a facility's security protection system. The code has been extensively tested on sample accounting systems and subsets of material control systems.

Some computational difficulties arise when we apply the code to material control data which reflect a complex system involving added and virtual tamper protection. When a tamper protection system protects not only the component in question but its supporting components also, then the monitors are virtually self-protected. If, for example, the receiver of a CCTV goes blank because the power supply to that CCTV has been tampered with, that fact is an indication that something is wrong. The high degree of complex connectivity between the elements of such a system requires prohibitively large amounts of computer time and storage space to do the analysis, thus placing a fairly severe limit to the size of the facilities which can be evaluated. Several approaches to the problem of size limits for the tampering analysis code are being developed. They include a partitioning algorithm, methods of data storage, and consolidation of elements.

2.3.2.1 Partitioning Algorithm. The partitioning algorithm under development divides large blocks of data into smaller sections which can be solved

independently. Components whose connections are entirely local to the block can be eliminated and only those components with more global connections must be carried over to the next block. This technique could be applied successfully to very large facilities. The code development of the partitioning algorithm is about 90% complete[1].

2.3.2.2 Methods of Data Storage. The connections between components as defined by the reachability matrix have been keyed in the computer by multiples of prime numbers. This technique is very successful in storing large numbers of components with relatively few connections, as is typical for an accounting system. An alternate storage scheme using bit vectors proves more advantageous for highly connected matrices and allows much faster manipulation of the data, but is more limited in the total number of components which can be handled. Converting the tamper analysis code to bit vector data storage has allowed substantial reduction in the amount of time necessary to do the reachability analysis on the CDC-7600 computer. Further discussions of the bit vector approach will be included in forthcoming reports.

2.3.2.3 Consolidation Of Components. Decreasing the number of components, or nodes, in a matrix dramatically decreases the amount of computer time to run a problem. A condensation algorithm is being developed which will combine two nodes if they

- are unconditionally bi-directionally connected regardless of other connections,
- are unconditionally, uni-directionally connected, provided the receiving node has no other entries,
- have identical entries regardless of the exit pattern, or
- have identical exits regardless of the entry pattern.

In addition, source nodes, those which have no entries to them, may be removed during the reachability calculation and restored later, as they will not affect the interior connections.

2.3.2.4 Computer Resource Requirements

Some preliminary tests have been performed to determine the computer time requirements. Since the coding for the condensation algorithm was not as yet complete, we were able to test the reachability calculation by performing certain operations without using the computer. For example, by condensing the test data by hand, we were able to perform the reachability calculation in one-tenth the original time.

During the coming quarter, the condensation algorithm and some input/output routines will be implemented in the code.

3.0 DEVELOPMENT OF VALUE-IMPACT METHODOLOGY

Contributors: R. Al-Ayat, J. Huntsman**, B. Judd**

As delineated in the current draft of the MC&A Upgrade Rule, the performance of a material control and accounting system is to be evaluated in terms of three standards: detection, response, and confirmation. Our work on the Value-Impact Modeling tasks this quarter emphasized the MC&A response function and to a limited extent the confirmation objective. The following is a brief description of our approach to modeling the response/resolution process for alarms generated by an MC&A system.

We consider two facets of alarm resolution: 1) resolving the status of SSNM and 2) determining the cause (i.e., the initiating event) of the alarm. Our primary focus is on resolving the status of SSNM. Two resolution states are possible: Material Accounted For (MAF) or Material Unaccounted For (MUF). In this report MUF states include material misplaced (not accounted for, but not diverted) and material missing (diverted).

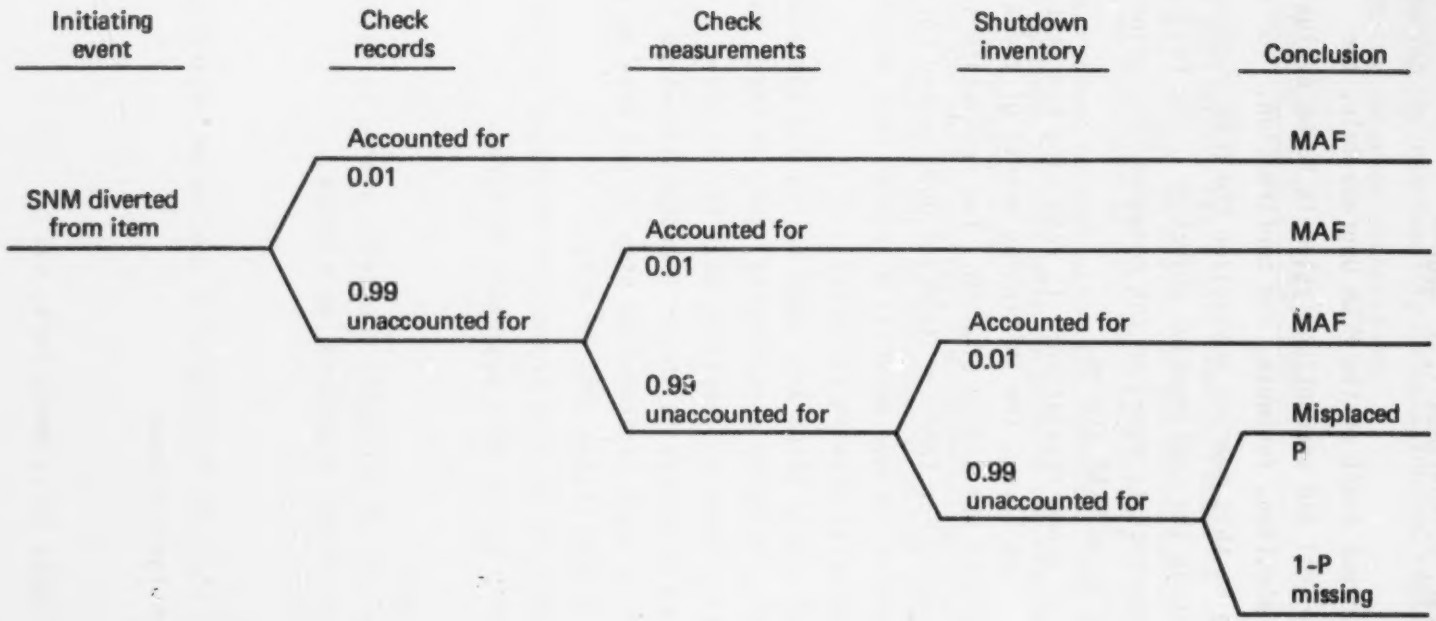
Once an MC&A alarm occurs, many steps are taken to resolve the alarm. These include checking records, checking measurements, and, if these do not account for the alleged missing material, shutting down for physical inventory. A typical sequence of events is shown in probability-tree format in Fig. 1. At the completion of each intermediate step in the tree we assume a conclusion is reached as to SSNM status (MAF or MUF).

The adequacy of these alarm resolution procedures is judged in the value-impact analysis according to two main aggregate measures.

1. P(Correct resolution)
   This is the probability of correctly resolving alarms to determine SNM status: accounted for, misplaced, or missing.

2. E(Time to resolve)
   Expected time from alarm to issuance of a conclusion regarding SNM status by the investigative team.

**Applied Decision Analysis (ADA) Inc., Menlo Park, Ca.



Notes:
- MAF = Material Accounted For
- (P) and (1-P) are computed from alarm frequency data
- Numbers are for illustration purposes only

Fig. 1. Probability tree for sample resolution process

We can break down these aggregate resolution measures to finer levels of detail. That is, the performance measures can be conditioned on the quantity of SNM involved or the alarm initiating event (e.g., communicated threat, internal alarm, or error condition). Also, we can compute the accuracy for each type of conclusion.

One of the problems involved in computing the above aggregate measures of performance is the need for data on the occurrence rates of false alarms. For our purpose, we consider only those false alarms identical to true indications by the MC&A system that SSNM is misplaced or missing e.g., material missing from an item or material missing from a process.

We developed two procedures for eliciting the frequency of these false alarms:

- elicit underlying causes of alarms and their frequency
- elicit directly the false alarm frequency.

The steps in the modeling approach are: enumerating the underlying causes for alarms, then assessing the frequency of these causal events, and from this data computing false alarm frequency. This modeling approach is the best procedure to use when false alarms occur infrequently, especially when they can only occur as the result of multiple failures or mistakes. On the other hand, the direct approach is best when data on false alarm frequencies exists, because less time is required than for the modeling approach.

The modeling approach is illustrated in Table 1. Nine causes of alarms are indicated; these are grouped into human errors and measurement errors. The row totals represent the overall frequency of each cause and the column totals give overall frequencies for each alarm type, which are the desired false alarm rates.

These performance measures for the resolution function form an integral part of the MC&A system effectiveness evaluation. Data is being collected from personnel at an operating facility to evaluate the effectiveness of a baseline system designed in compliance with the current MC&A regulations governing the detection and resolution of safeguards alarms. This baseline system evaluation is then used to assess the cost-effectiveness of the recommended MC&A Upgrade Rule.

Table 1. Illustrative false alarm frequency data (alarms per year)

Cause	Alarm type: SNM from item	Item from vault	SNM from process	Cause total
MEASUREMENT ERRORS				
1. Holdup*	0	0	2.0	2.0
2. Spill*	0	0	0.25	0.25
3. Sample error	0.6	0	2.4	3.0
4. Miscalibration	0.02	0	0.08	0.1
HUMAN ERRORS				
5. Can misplaced	0	1.0	0	1.0
6. Misrecorded transfer	0	0.24	0.96	1.2
7. Item mislabelled	0.5	1.5	1.0	3.0
8. Transcription error	0.5	1.5	1.0	3.0
9. Calculation error	0	0	0.3	0.2
ALARM TOTAL	1.6	3.7	6.9	12.2

*Greater than limit of error.

4.0 DEVELOPMENT OF IMPROVED GUIDANCE CAPABILITIES FOR MC&A SYSTEMS

Contributors: P. Chilton,* D. Dunn, G. Kufahl,* J. McDonnel,* A. Vergari*

This task is a follow-on effort to an FY79 task devoted to a systematic evaluation and critique of the current material accounting regulations. Both were motivated by the April 1978 NRC MC&A Task Force Report[6], which identified weakness in current material accounting systems.

The purpose of this task is to develop or recommend 1) concepts, principles, and methods for protecting material accounting (MA) data from falsification, 2) MA checks and balances for detecting theft or diversion, and 3) MA organizational criteria which support safeguards effectiveness.

Our FY79 work led to the development of a generic, minimal material accounting (GMMA) system and its associated information flow diagrams.[7] The GMMA system is representative of a typical MA system, and it is minimum in the sense that it contains no safeguards or accounting elements in excess of those required by regulation.

Subsequent analysis identified all possible vulnerability event sets and all possible protective path sets for a Bulk Theft and an Item Theft scenario. The vulnerability event sets defined the minimal set of safeguards accounting elements (e.g., reports, records, documents, measurements, controls, consistency checks) which, if accessed and tampered with, could defeat the detection mechanisms of the GMMA system. On the other hand, protection path sets are sets of accounting elements which must be protected or controlled in order to make the GMMA system invulnerable to tampering. By definition, a protective path set will contain at least one element of each vulnerability set.

---

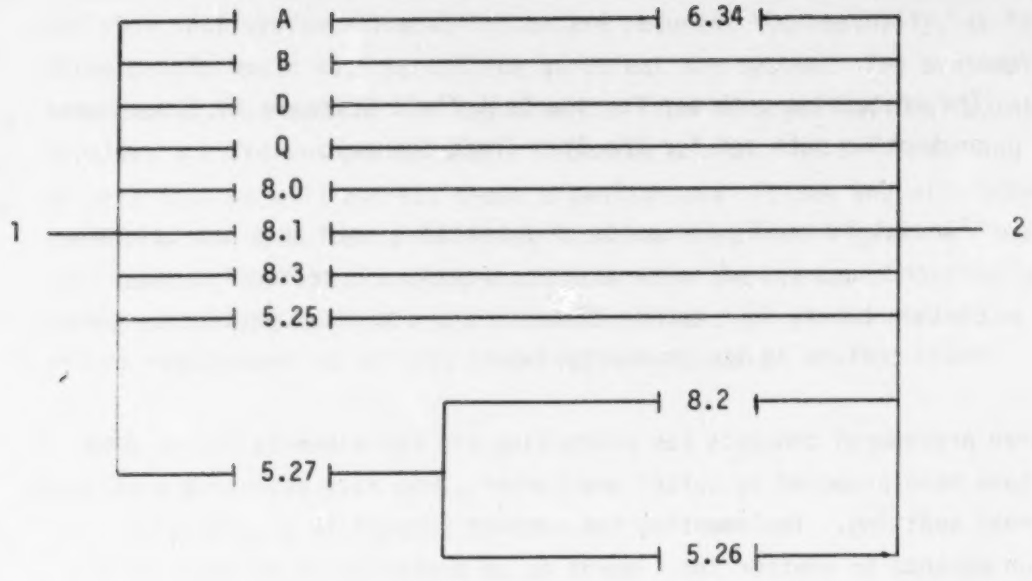
*Advanced Technology Associates (ATA), Inc., Dublin, California

We are using as a basis for our present work the GMMA system, its vulnerability event sets, and its protective path sets. Bottom-up and top-down approaches are being used to address the above issues. In the bottom-up approach upgrades or changes based upon current material accounting practices that are more than minimally required are being examined. The top-down approach, on the other hand, will result in suggested upgrades based principally upon auditor experience and from consideration of the protective path sets.

Vulnerability events for the three loss detection procedures (Item Count, Item Quantity, and Inventory) contained in the GMMA system were represented graphically (like electronic series and parallel circuits). As a result all vulnerability events, including the minimum event sets, and the many possible associated protective path sets, can be visualized.

To illustrate our approach, Fig. 2 shows the vulnerability event set circuit for the GMMA Item Count Procedure (ICP), where the circuit elements represent specific facility item control records, reports, documents, etc.[7] The circuit has a starting point denoted by 1 and an ending point denoted by 2. The tampering of any path from point 1 to point 2 potentially can defeat the Item Count Procedure detection mechanism and therefore represents a vulnerability event. The Item Count Procedure has 15 vulnerability events defined by all possible paths from point 1 to point 2; the set of all 15 events denotes the Item Count Procedure vulnerability event set. This set represents all possible ways that the Item Count Procedure can be "defeated" and indicates which combination of records, reports, documents, etc., must be accessed to defeat the detection system.

Again, a protective path set will contain at least one element of each vulnerability event. The elements of a protective path must be 'protected' to preclude the possibility of theft of SNM material. Protective path sets for the Item Count Procedure are evident from Figure 2. A minimal protective path set contains the least number of elements which completely protects the Item Count Procedure. In this case three minimal protective path sets exist with twelve elements each.



A = 3.11 * 3.17

B = 6.34 * (6.24 + 5.24 * 5.27)

D = 6.15 + 6.16 + 6.40 + 8.4 * 8.10 * 8.11

Q = 5.4 + 5.21

where * is a logical AND and + is a logical OR.

Fig. 2. The Item Count Procedure Vulnerability Event Set Circuit. (Numbers refer to specific records, documents, and reports of the GMMA system found in reference 2.)

The graphical analysis of the GMMA system established two important facts:

- The protective path set for the Bulk Theft Scenario includes the protective path set for the Item Theft Scenario.

- Although literally thousands of protective path sets are possible for the hundreds of vulnerability events, all protective sets contain twenty-four common elements and a minimal protective path could contain as few as thirty-two.

Three procedural concepts for protecting the key elements in the GMMA system have been proposed by Kufahl and Vergari, who have extensive experience in internal auditing. Implementing the correct concept in a particular situation depends on whether the element to be protected is an input to a report or document, a control element, or a procedure response element. The method of protecting elements other than controls or procedure response elements is called Skip Echelon Verification and requires that duplicate information be forwarded one echelon ahead of the normal recipient. The end result is to eliminate a particular report or document element from the vulnerability event set. For control elements, a set of rules were formulated which control the process of altering prescribed methods of procedure. They are thus Control on Controls. These simple rules, when implemented, would dictate that controls could be defeated only through the involvement of three or more individuals acting in collusion. The procedure response elements are protected by the simple mechanism of Secondary Echelon Reporting, which requires duplicate information to be forwarded to NRC by the producers of the data that is provided to the nominal responder. This data can then be compared with the response normally forwarded and then be discarded. Skip Echelon Verification, Control on Controls, and Secondary Echelon Reporting are thus recommended upgrade procedures.

We have applied these three procedural concepts to the GMMA system and can show that system vulnerabilities are reduced. Conceptually, at least three people would have to collude to defeat the system. The presumption, however, is that each of the key elements from an organizational point of view involves a different person and/or separate access. In the remaining effort of this Task we will address these organizational issues and will attempt to develop planning criteria for those features that have significant safeguards implication. Follow-on effort would determine the impact of the implementation of these procedures on specific licensees and determine the added effort requirement to enforce their implementation.

5.0 ANALYSIS OF THE ROLE OF AN INTERFACILITY SNM ACCOUNTING SYSTEM FOR NRC SAFEGUARDS ASSURANCE

Contributors: D. Dunn, J. McDonnel,* and R. Mullen*

The primary purpose of this task is to analyze the actual and potential value/impact of an interfacility NRC material accounting system involving information flows between licensed facilities, NRC headquarters, NRC regional offices and the DOE/NRC Nuclear Material Management Safety and Safeguards (NMMSS) facility at Oak Ridge, Tennessee. Value is measured in terms of safeguards effectiveness, including strengths and weaknesses in deterring or detecting both material diversion and facility material accounting falsification. Impact is measured in terms of reporting requirements which the NRC may impose upon the licensees.

The primary objectives of this task in view of the above are threefold:

- Characterize current national MC&A information flows and corresponding detection mechanisms
- Identify accounting checks and audits which could be employed using currently available data
- Determine additional data needs and corresponding safeguards checks and auditing mechanisms.

Progress to date has focused on collecting and reviewing narrative descriptions of the Safeguards Status Report System (SSRS) and the NMMSS. In addition, extensive interviews were conducted with NRC Region 5 personnel to clarify our understanding of the SSRS and with Boeing Computer Services personnel familiar with the NMMSS. Interviews are planned with individuals at NRC headquarters and at Oak Ridge, Tennessee.

*Advanced Technology Associates (ATA) Inc., Dublin, California

An initial evaluation of the SSRS has included analyzing its relationship to the Code of Federal Regulations, understanding its data acquisition and input, identifying the timeliness of information, and analyzing its relationship to the NMMSS.

6.0 REFERENCES

1. Donald Dunn, Safeguards Material Control and Accounting Program: Quarterly Report, October-December, Lawrence Livermore National Laboratory, Livermore, CA., UCRL 52715-80-1, NUREG/CR 1485 Vol I, No.1 (1979).

2. U.S. Nuclear Regulatory Commission, Fixed Site Physical Protection Upgrade Rule Guidance Compendium, Volume I, NUREG 0669 Vol I (1980)

3. A. A. Parziale, D. J. Ross and I. J. Sacks, The License Submittal Document and Format for Material Control and Accounting Assessment, Vol. II, Lawrence Livermore National Laboratory, Livermore, CA, UCRL-52735, NUREG/CR-1233, (1979). (To be published November 1980)

4. A. A. Parziale and I. J. Sacks, Data Requirement Comparison Between the Fixed Site Upgrade Rule Guidance Compendium and the Structured Assessment Approach License Submittal Document, Lawrence Livermore National Laboratory, Livermore, CA, UCID-18671 (1980).

5. I. J. Sacks, A. A. Parziale, D. W. Freeman, C. J. Patenaude, P. A. Renard, and D. J. Ross, Computational Package: The Structured Assessment Approach Version 1, Lawrence Livermore National Laboratory, Livermore, CA, UCID-18146 (1980). Section 2.8

6. United States Nuclear Regulatory Commission, Report of the Material Control and Material Accounting Task Force, NUREG-0450 (1978).

7. J. Lim and J. Huebel, Material Accounting As Required by the U.S. Nuclear Regulatory Commission: Capabilities and Vulnerabilities, Lawrence Livermore National Laboratory, Livermore, CA, UCRL-52734, NUREG/CR 1192 (1980).

NRC FORM 335 (7-77) U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER (Assigned by DDC)
NUREG/CR-0849, Vol.1 No.2
UCRL-52715-80-2

4. TITLE AND SUBTITLE (Add Volume No., if appropriate)
Safeguards Material Control and Accounting Program: Quarterly Report, January-March 1980

2. (Leave blank)

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
Andrew J. Poggio and Donald R. Dunn

5. DATE REPORT COMPLETED
MONTH September YEAR 1980

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Lawrence Livermore National Laboratory
NSS Safeguards Program, L-97
P.O. Box 808
Livermore, CA 94550

DATE REPORT ISSUED
MONTH October YEAR 1980

6. (Leave blank)

8. (Leave blank)

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Safeguards, Fuel Cycle & Environmental Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.
FIN No. A0115

13. TYPE OF REPORT
NUREG

PERIOD COVERED (Inclusive dates)

15. SUPPLEMENTARY NOTES

14. (Leave blank)

16. ABSTRACT (200 words or less)

This report summarizes the activity of the Safeguards Material Control Accounting Program (MC&A) during the January-March 1980 quarter, conducted for the U.S. Nuclear Regulatory Commission at Lawrence Livermore National Laboratory. Described is progress made in the continued development of the Structured Assessment Approach (SAA) vulnerability methodology, particularly in preparing a user-oriented input-output interface and reducing the SAA's computer resource requirements. Also, a newly initiated technology transfer effort in which the NRC staff participated is detailed. Work continued in developing a value-impact methodology that focused on modeling alarm resolution; specifically, the procedures developed for eliciting the frequencies of false alarms are described. Additional support of the MC&A Upgrade Rule development, namely, analyzing the vulnerabilities of a generic minimal material accounting system to establish guidelines and checks and balances to prevent data falsification, is presented and a graphical procedure used in this effor is described. The report concludes with a brief description of the initial work performed in analyzing the role of an interfacility accounting system for safeguards assurance.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS (This report)
Unclassified

21. NO. OF PAGES
25

20. SECURITY CLASS (This page)
Unclassified

22. PRICE
$

NRC FORM 335 (7-77)

25/0849/V.1/no. 2/errata

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

NEWARK PUBLIC LIBRARY

FEB 27 1981

U. S. GOVT. PUBS.
DEPOSITORY 376

November 25, 1980

ERRATA SHEET

for

NUREG/CR-0849, Vol. 1, No. 2

SAFEGUARDS MATERIAL CONTROL AND ACCOUNTING PROGRAM:
QUARTERLY REPORT, JANUARY-MARCH 1980

Performed by

Lawrence Livermore National Laboratory

for the

U.S. Nuclear Regulatory Commission

Please make the following correction to the report number:

Change: NUREG/CR-0849, Vol. 1, No. 2

To: NUREG/CR-0849, Vol. 2, No. 1

DIVISION OF TECHNICAL INFORMATION

AND

DOCUMENT CONTROL

Y 3.N88:

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
U.S. NUCLEAR REGULATORY
COMMISSION

NUREG/CR-0849, Vol 1, No. 2

SAFEGUARDS MATERIAL CONTROL AND ACCOUNTING PROGRAM:
Quarterly Report, January–March 1980

October 1980